



Intakeadvies NL Gov Assurance Profile for OAuth 2.0 versie 1.1

Vergadering:	Forum Standaardisatie woensdag 24 september 2025
Agendapunt:	
Documentnummer:	
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	29 augustus 2025
Versie:	0.9
Bijlagen:	geen
Rechten:	CC0 publieke domein verklaring

1 Samenvatting en advies

De Stuurgroep Open Standaarden adviseert het Forum Standaardisatie om de versie 1.1 van de standaard NL Gov Assurance profile for OAuth 2.0 in procedure te nemen voor plaatsing op de 'Pas toe of leg uit'-lijst. Een verkort expertonderzoek is aangewezen om de nieuwe versie van de standaard te toetsen aan de criteria voor opname op de lijst.

Tijdens de intakeprocedure kwamen de volgende bijzonderheden naar voren:

- duidelijkheid en duurzaamheid van de naamgeving
- duiding van welk relevant/bestaand probleem de nieuwe versie oplost
- de indiener heeft tijdens de intake de wens voor het predicaat Uitstekend beheer uitgesproken
- adoptie en betrokkenheid van organisaties uit het organisatorisch toepassingsgebied
- impact van het verplichten van het NL-profiel op de onderliggende standaard die nu op de Aanbevolen-lijst staat
- aankomende versies (1.2/2.0) die Logius beoogt aan te melden voor de 'Pas toe of leg uit'-lijst
- opvolging van de adoptieadviezen uit het [Forum-advies](#) van 2020

In de rest van dit document wordt het advies nader onderbouwd. Hoofdstuk 2 geeft een korte uitleg van de standaard. Hoofdstuk 3 beschrijft het proces waarmee dit advies tot stand kwam, alsmede de vervolgstappen. Hoofdstuk 4 toetst in hoeverre de standaard voldoet aan de criteria om in behandeling genomen te worden door het Forum Standaardisatie. Hoofdstuk 5 verkent of er inhoudelijke belemmeringen bestaan die een positief expertadvies in de weg zouden kunnen staan.

Tot slot wordt er in hoofdstuk 6 een praktijkvoorbeeld gegeven dat Forum Standaardisatie kan gebruiken om de maatschappelijke meerwaarde van het toepassen van de standaard te communiceren.

2 Korte beschrijving van de standaard

2.1 Over de standaard

De standaard [NL Gov Assurance profile for OAuth 2.0](#) legt bindende afspraken vast over hoe de [International Government Assurance Profile for OAuth 2.0](#) (OAuth 2.0, [geplaatst](#) op de lijst aanbevolen standaarden) moet worden toegepast binnen de Nederlandse overheid. NL Gov Assurance profile for OAuth 2.0 is een Nederlands profiel op de internationale standaard OAuth 2.0.

Met NL Gov Assurance profile for OAuth 2.0 kunnen gebruikers een website of webapplicatie autoriseren om hun persoonlijke gegevens via een REST API op te halen bij een ander systeem, zonder daarbij hun gebruikersnaam en wachtwoord uit handen te geven. NL Gov Assurance profile for OAuth 2.0 legt nadere afspraken vast over het gebruik van OAuth 2.0 bij de Nederlandse overheid. Zo bepaalt de standaard hoe applicaties zich bij elkaar moeten registreren en hoe autorisatiecodes veilig moeten worden uitgewisseld. OAuth 2.0 laat daarin namelijk nog te veel implementatie opties vrij.

De nieuw aangemelde versie (1.1) van deze NL Gov Assurance profile for OAuth 2.0 is een kleine, incrementele update ten opzichte van de vorige versie. De belangrijkste toevoeging is dat systemen die geen gebruik maken van user OAuth (bijvoorbeeld geautomatiseerde systemen zonder tussenkomst van een eindgebruiker) op een gestandaardiseerde manier toegang kunnen krijgen tot gegevensbronnen. Dit vergroot de interoperabiliteit en herbruikbaarheid van overheidsdata, en maakt het eenvoudiger voor systemen om met elkaar samen te werken.

2.2 Waarom is deze standaard belangrijk?

Het nut van de nieuwe versie (1.1) ligt in het verbeteren van interoperabiliteit van en veiligheid van authenticatie en toegang tot gegevensbronnen. De vernieuwde functies van NL Gov Assurance profile for OAuth 2.0 versie 1.1 maken het mogelijk om binnen het bestaande profiel gegevens veilig uit te wisselen - zowel nationaal als internationaal, en zowel client-2-machine als machine-2-machine.

3 Betrokkenen en proces

Op 20 december 2024 heeft Logius het NL Gov Assurance profile for OAuth 2.0 versie 1.1 aangemeld voor plaatsing op de 'Pas toe of leg uit' lijst. Omdat het om een beperkte versiewijziging gaat, is afgestemd de besluitvorming van het Forum Standaardisatie en het OBDO af te wachten over [het voorstel](#) (thans geaccordeerd) om de procedures voor beperkte versiewijzigingen te verkorten. Op 14 augustus 2025 heeft een intakegesprek plaatsgevonden met de indiener, procedurebegeleider InnoValor Advies en Bureau Forum Standaardisatie. Bij het (online) intakegesprek waren de volgende personen aanwezig:

- Mironov, Stas (Logius)
- De Jongh, Cigdem (InnoValor Advies B.V.)
- Vermeulen, Claudia (InnoValor Advies B.V.)
- Kobes, Wouter (Bureau Forum Standaardisatie)
- Verspaget, Joram (Bureau Forum Standaardisatie)

In dit gesprek is onderzocht of NL Gov Assurance profile for OAuth 2.0 versie 1.1 voldoet aan de criteria om in procedure te worden genomen. Daarnaast is vooruitgeblikt op de procedure. Dit intakeadvies is tot stand gekomen op basis van het intakeonderzoek.

4 Voldoet de standaard aan de criteria om in procedure genomen te worden?

NL Gov Assurance profile for OAuth 2.0 versie 1.1 voldoet aan alle [vier criteria](#) om in behandeling genomen te worden voor plaatsing op de 'Pas toe of leg uit' lijst. Hoe de standaard is getoetst op de vier criteria wordt hieronder toegelicht in paragrafen 4.1-4.4.

4.1 Valt de standaard binnen de scope van Forum Standaardisatie?

Criterium: "Het opnemen van de standaard op de lijst dient in substantiële mate bij te dragen aan het bevorderen van de interoperabiliteit, van een toekomstbestendige gegevensopslag en/of van een verminderde leveranciersafhankelijkheid."

Ja, de standaard draagt bij aan het bevorderen van interoperabiliteit en veiligheid van gegevensuitwisseling voor Nederlandse overheden en instellingen uit de (semi-)publieke sector. Door afspraken vast te leggen over het gebruik van OAuth zorgt NL Gov Assurance profile for OAuth 2.0 versie 1.1 voor veilige uitwisseling van autorisatiecodes. Ook kunnen systemen die geen gebruik maken van user OAuth op een gestandaardiseerde manier toegang krijgen tot gegevensbronnen.

4.2 Heeft de standaard een toepassing die een enkele organisatie of sector overstijgt?

Criterium: "Het beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied van de standaard dient voldoende breed te zijn en betrekking te hebben op gebruik door de (semi-)overheid."

Ja, het beoogde functioneel toepassingsgebied en het organisatorisch werkgebied van de standaard NL Gov Assurance profile for OAuth 2.0 versie 1.1 is voldoende breed om substantieel bij te dragen aan de interoperabiliteit van de (semi-)overheid. De toepassing van de standaard overstijgt een enkele organisatie of sector. De standaard NL Gov Assurance Profile for OAuth 2.0 versie 1.1 wordt toegepast bij applicaties waarbij gebruikers of 'resource owners' – expliciet of impliciet toestemming geven aan een derde partij om namens hen toegang te krijgen tot gegevens via REST API's waarvoor zij bevoegd zijn. Dit geldt zowel voor client-2-machine- als machine-2-machine-communicatie.

4.3 Is de standaard al wettelijk verplicht?

Criterium: "Het uitvragen of gebruiken van de standaard moet niet al verplicht zijn op grond van een bestaande (Europees) wettelijke verplichting die gelijk dan wel groter is dan het voor de lijst beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied."

Nee, de standaard is niet al wettelijk verplicht. NL Gov Assurance profile for OAuth 2.0 is 15 juli 2019 opgenomen op de 'Pas toe of leg uit'-lijst van het Forum Standaardisatie. De achterliggende standaard OAuth 2.0, die op de lijst aanbevolen standaarden van het Forum Standaardisatie staat, heeft eveneens geen wettelijke verplichting.

4.4 Draagt de standaard bij tot de oplossing van een bestaand, relevant probleem?

Criterium: "De standaard dient bij te dragen aan de oplossing van een bestaand, relevant probleem."

Ja, de standaard draagt bij tot de oplossing van een bestaand, relevant probleem. De herziene opmaak in NL Gov Assurance profile for OAuth 2.0 versie 1.1 maakt duidelijk welke content specifiek Nederlands is en welke content nog overeenkomt met de internationale basis (OAuth 2.0). Ook draagt de toevoeging van het client credentials profiel bij aan de interoperabiliteit van systemen omdat ook systemen zonder 'user OAuth' (bijvoorbeeld geautomatiseerde systemen zonder tussenkomst van een eindgebruiker) veiliger toegang krijgen tot een gegevensbron.

5 Is er zicht op een positief expertadvies?

Ja, er is zicht op een positief expertadvies. Het intakeonderzoek heeft geen inhoudelijke bezwaren opgeleverd die een positief expertadvies voor plaatsing van NL Gov Assurance profile for OAuth 2.0 versie 1.1 op de 'Pas toe of leg uit'-lijst in de weg zou kunnen staan.

Als het Forum Standaardisatie de standaard in procedure neemt, gaat een groep experts de standaard toetsen op de [vier inhoudelijke criteria](#) voor opname op de 'Pas toe of leg uit'-lijst. Het Forum Standaardisatie neemt geen standaarden in procedure waarvan bij aanvang al vaststaat dat deze niet op een positief expertadvies kan rekenen. Daarom wordt in dit intakeadvies vooruitgeblikt op de vier inhoudelijke criteria. Dit wordt toegelicht in paragrafen 5.1-5.4.

5.1 Toegevoegde waarde

NL Gov Assurance profile for OAuth 2.0 versie 1.1 levert een duidelijke en uitlegbare interoperabiliteitswinst op. Door duidelijk onderscheid te maken tussen wat specifiek Nederlands is en wat internationaal toepasbaar is, sluiten Nederlandse oplossingen beter aan bij de rest van Europa en daarbuiten. Daarnaast is een nieuw profiel toegevoegd (client credentials profiel) dat ook systemen zonder gebruikers inlog (user OAuth) toegang kan geven tot gegevensbronnen. Dit vergroot de mogelijkheid om processen efficiënter te automatiseren en diensten betrouwbaarder en veiliger aan te bieden. In de [Github repository](#) zijn ook werkversies, besluitvorming, logboeken en de '[releases](#)' inzichtelijk, zodat precies te volgen is welke wijzigingen zijn doorgevoerd en op basis waarvan.

De baten van adoptie wegen zowel maatschappelijk als voor de overheid op tegen de mogelijke kosten en risico's. De implementatie van de standaard zal kosten met zich meebrengen, maar deze zijn naar inschatting acceptabel. De implementatie van de standaard zal naar verwachting geen risico's hebben mits de standaard strikt volgens de regels wordt geïmplementeerd.

De standaard overlapt niet met bestaande standaarden op de lijst en conflicteert ook niet. De standaard sluit aan op de voorgaande versie (1.0) en op de internationale standaard OAuth 2.0. Er zijn geen concurrerende open standaarden bekend die dezelfde functionele en organisatorische scope hebben. Tot slot brengt NL Gov Assurance profile for OAuth 2.0 versie 1.1 geen significante veiligheids- of privacyrisico's met zich mee.

5.2 Open standaardisatieproces

De standaard NL Gov Assurance profile for OAuth 2.0 wordt beheerd door Logius. Het volledige [beheerproces](#) is gedocumenteerd en is voor eenieder vrij toegankelijk. Het [specificatiedocument](#) van de standaard is kosteloos beschikbaar, evenals aanvullende documentatie over het ontwikkel- en beheerproces, die openbaar wordt gedeeld via de GitHub. In de [GitHub repository](#) zijn ook overleggen en besluitvorming inzichtelijk, zodat precies te volgen is welke wijzigingen zijn doorgevoerd en op basis waarvan. Het beheer van de standaard valt onder de financiering die de beheerder (Logius) ontvangt van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Logius organiseert vier keer per jaar technische overleggen over het beheer en doorontwikkeling van de standaard met partijen als de gemeente Den Haag, de Rijksdienst voor Identiteitsgegevens (RvIG), de Dienst Uitvoering Onderwijs (DUO), Kennisnet en Kadaster. Ook organiseert Logius werkgroep bijeenkomsten bij het Kennisplatform API's voor

belanghebbenden, (semi-)overheidsorganisaties zoals Kamer van Koophandel (KvK), Kadaster, DUO, RINIS, Geonovum en VNG om ervaringen op te halen bij partijen die de standaard implementeren. Hier wordt kennisgenomen van implementatieknelpunten van het profiel en worden wijzigingsvoorstellen (RFC's) beoordeeld wanneer deze stabiel zijn en de veiligheid of efficiëntie kunnen bevorderen.

Partijen die zich aanmelden en aantonen dat zij belang hebben bij de standaard worden ook uitgenodigd om deel te nemen aan het beheerproces. Logius vraagt aan de leden van het Technisch Overleg hun implementaties te melden en draagt tevens op verzoek de bij haar bekende gebruiksgegevens aan voor de Monitor open standaarden van Forum Standaardisatie.

De standaard valt onder een [Creative Commons Attribution 4.0 License](#). Dit betekent dat het werk onder de volgende voorwaarden mag worden gedeeld en gebruikt: bronvermelding, link naar licentie, wijzigingen vermelden.

5.3 Draagvlak

NL Gov Assurance profile for OAuth 2.0 versie 1.1 lijkt op voldoende breed draagvlak te kunnen rekenen binnen de overheid. Een voorwaarde hierbij is ook dat er voldoende marktondersteuning voor de standaard bestaat en dat het marktaanbod evenwichtig is (dus geen leveranciersafhankelijkheid in de hand werkt).

Verschillende overheidsorganisaties maken gebruik van NL Gov Assurance profile for OAuth 2.0 versie 1.1, zoals de gemeente Den Haag, Kadaster, de Politie en Logius. Eerdere versies van de standaard worden nog gebruikt binnen de overheid door onder andere Kadaster, DUO en Logius. Doordat de nieuwe versie (1.1) backward compatible is met versie 1.0 wordt de comptabiliteit tussen de nieuwe en eerdere versie in de praktijk geborgd. Er is voor de implementatie van NL Gov Assurance profile for OAuth 2.0 versie 1.1 voldoende marktondersteuning. De standaard een profiel is op het International profiel OAuth 2.0 wat veel wordt gebruikt en heeft daarom zowel Nederlandse als Internationale leveranciers zoals [Okta](#), [Authlete](#) en [Ory](#).

Er zijn geen aanvullende afspraken nodig om de standaard te kunnen toepassen. De standaard beschikt niet over een conformiteitscheck. Omdat NL Gov Assurance profile for OAuth 2.0 versie 1.1 een profiel is op een Internationale standaard zijn er voldoende use cases beschrijvingen van de 'client credential flow' en 'authorization code flow' beschikbaar via [Digitale overheid](#). De beheerder biedt zelf geen voorbeeldimplementatie van de standaard.

5.4 Opname op de lijst bevordert adoptie

Het verplichten of aanbevelen van NL Gov Assurance profile for OAuth 2.0 versie 1.1 lijkt te kunnen bijdragen aan de adoptie van de standaard door de overheid. De standaard is een profiel op de Europese standaard OAuth 2.0. Opname op de 'Pas toe of leg uit'-lijst van voorgaande versies biedt overheden een houvast om en een duidelijk signaal dat OAuth 2.0

de te verkiezen standaard is. De voorgaande versie staat dan ook op de 'Pas toe of leg uit'-lijst. De opname versie 1.1 verbetert niet alleen de positie van gebruikers, maar bevordert ook de interoperabiliteit en veiligheid van de standaard.

Logius, als beheerder, pakt vragen en issues betreffende de standaard op, maar ondersteuning van implementatie gebeurt vaak in-house of wordt door marktpartijen aangeboden. Naast de normatieve standaard wordt ook een informatief document beschikbaar gesteld waarin praktijkvoorbeelden en een leeswijzer (potentiële) gebruikers op weg helpen.

6 Praktijkvoorbeeld

Zodra je bent ingelogd met [DigiD](#) voor het aanvragen van een parkeervergunning via een app van de gemeente wordt er in de backend een token exchange gedaan. Deze token exchange zorgt ervoor dat je authenticatie token van [SAML](#) naar OAuth wordt omgezet. Deze token kan je dan 'natively' meesturen met een 'API call; richting de Rijksdienst voor Wegverkeer (RDW) bijvoorbeeld. In het token geef je toestemming en bewijs van inloggen mee zodat de RDW 'resource server' de gegevens van je motovoertuig (bijv. kenteken) kan delen met de gemeente. Omdat dit OAuth is en volgens NL Gov geïmplementeerd wordt, hoeven de partijen niks van elkaar te weten wat betreft OAuth. De token is interoperabel en 'self-contained'. Bovendien is het extra veilig als je de 'advanced security measures' uit het NL Gov Assurance profile for OAuth 2.0 versie 1.1 gebruikt.